prego. IaaS

Die neue Realität für Ihr Enterprise Network

Die neuen Herausforderung im Netzwerk

1. Corporate Network/Büronetzwerk – Zugang zu einem modernen Workplace

Der Workplace befindet sich im Wandel – die digitale Transformation beginnt am Arbeitsplatz
Der Mittelstand beschäftigt sich mit neuen Märkten, was eine moderne und zukunftweisende Netzwerkinfrastruktur erfordert. Bisher eingesetzte Büronetzwerke sind oft für die neuen Herausforderungen wie Mobilität, Cloud Services und Netzwerksicherheit nicht optimal aufgestellt. Flexible Netzwerke, bei denen das „Secure by Design"-Prinzip von Anfang an durchgängig umgesetzt ist, werden benötigt.

Wie setzen wir solche Themen konkret um?
Mit verschiedenen Kunden werden bei uns bereits Visionen für den Workplace der Zukunft entwickelt. Wenn klar ist, welche Anforderungen vorliegen, sind die Netzwerke so aufzubauen, dass der Mensch in der Benutzung später nicht eingeschränkt wird und sich neue Innovationen und Geschäftsfelder entwickeln können.

Durch Workshops mit den Kunden und Sichten von Dokumentationen wird schnell klar, welche Infrastrukturteile verbesserungswürdig sind. Gemeinsam wird eine neue zukunftweisende Infrastruktur konzeptioniert, realisiert und – falls gewünscht – auch betrieben.

2. Funktionsfähigkeit von kritischen Infrastrukturen

Welche neuen Herausforderungen bedingen die Schaffung von optimalen Netzwerkstrukturen in diesem Bereich?
Die Herausforderung ist, Netzwerke zu bauen, die einen Mindestsicherheitsstandard garantieren und erhebliche IT-Vorfälle erkennen und diese an das Bundesamt für Sicherheit in der Informationstechnik (BSI) melden.

Anders als bei Büronetzwerken sind Prozessnetzwerke statisch aufgebaut; man kennt die Kommunikationswege genau. Mit der Scada-Protokoll-Familie auf IP-Ebene wird das Management von industriellen Schaltgeräten oder Steuerungen durchgeführt.

prego. services

Neben einer geforderten hohen Verfügbarkeit ist den immer komplexer und ausgefeilter werdenden Cyber-Angriffsszenarien zu begegnen, während natürlich wohlbekannte „alte" Angriffe trotzdem nicht vernachlässigt werden können. Dadurch wird es notwendig, ständig weitere zusätzlichen Maßnahmen aufzuschichten, um ein Mindestmaß an Sicherheit garantieren zu können.

Zudem werden immer mehr Geräte in diesem Umfeld IP-fähig, welche vorher bspw. mit seriellen Anschlüssen gearbeitet haben. So werden auch immer mehr Geräte angreifbar. Digitalisierung und IoT sind hier die Schlagwörter.

Wie setzen wir solche Themen konkret um?
Wir arbeiten hier mit den zuständigen staatlichen Stellen und Institutionen eng zusammen, um über Bedrohungen stets auf dem aktuellen Stand zu sein und die eigenen Sicherheitsmaßnahmen fortlaufend evaluieren zu können. Ein Security-Expertenkreis ist im Notfall unabdingbar. Außerdem wird viel Zeit in die Weiterbildung und Produktentwicklung im Security-Bereich investiert, sodass wir – wie bisher – auch weiterhin schlüssige Konzepte für die sichere Anbindung von Prozessnetzwerken unterschiedlichster Art liefern können.

3. Fernwartung

Welche neuen Herausforderungen bedingen die Schaffung von optimalen Netzwerkstrukturen in diesem Bereich?
Im Umfeld kritischer Infrastrukturen sowie Büronetzwerken steht natürlich auch bei der Fernwartung die Sicherheit an erster Stelle. Eine standardisierte Fernwartung kann helfen, Kontrolle über die Remote-Zugänge zu behalten. Dies kollidiert jedoch oft mit den Usability-Anforderungen, die von den Endnutzern gestellt werden. Zudem kommt bei der Zwei-Faktor-Authentifizierung eine Vielzahl unterschiedlicher Verfahren zum Einsatz (RSA Token, Zertifikat, SMS Passcode). Neben starker Authentifizierung können – je nach Risikobetrachtung starker Verschlüsselung – Sprungserver, Aufzeichnungsserver und Zonenschnittstellen relevant für einen sicheren Fernwartungszugang sein.

Wie setzen wir solche Themen konkret um?
Um eine standardisierte Fernwartung zu konzeptionieren, ist zunächst eine Analyse aller Zugänge von außen in die betreffende Firma erforderlich.

Bei uns erfolgt zur Absicherung von Remote Access der Zugriff grundsätzlich über Sprungserver, wodurch mithilfe geeigneter Remote-Tools auch eine Aufzeichnung gewährleistet werden kann. Die Zonentrennung wird durch Sicherheitsgateways realisiert.

Selbstverständlich wird auch durch uns sichergestellt, dass aktuelle Verschlüsselungs- und Hashalgorithmen im Einsatz sind und eine Authentifizierung zwingend mit zwei Faktoren erfolgt.

4. Cloudservices – SAAS, IAAS

Welche neuen Herausforderungen bedingen die Schaffung von optimalen Netzwerkstrukturen in diesem Bereich?
Public Cloud Ressourcen werden immer beliebter, da sie flexibel und günstig nahezu beliebige Ressourcen zur Verfügung stellen können. Viele Unternehmen nutzen diesen Vorteil bereits. Unterschiedliche Branchen beispielsweise tun sich hier schwer, da der Umzug von Ressourcen „in die Cloud" stets mit einem gewissen Sicherheitsrisiko verbunden ist.

Dementsprechend müssen hier Lösungen gefunden werden, die es ermöglichen, zumindest den Zugriff auf Cloud Ressourcen abzusichern, da man in keinem Fall sichergehen kann, dass die Ressourcen für Außenstehende unzugänglich sind.

Wie setzen wir solche Themen konkret um?
Die Datenverbindung vom Coporate Network zur Cloud sollte zwingend verschlüsselt realisiert und – je nach Verfügbarkeitsanforderung – redundant ausgelegt werden. Sensible Daten dürfen bei Up- und Download nur über verschlüsselte Verbindungen gesendet werden. Je nach Sicherheitsniveau sollten die Daten in der Cloud verschlüsselt abgelegt werden, um die Vertraulichkeit zu gewährleisten. Wir konnten hierzu bereits in mehreren Projekten Erfahrungen sammeln. Sichere Verbindungen (siehe kritische Infrastrukturen) gehören zu unseren Kernkompetenzen.

Wir können Ihnen Planung, Realisierung und Betrieb einer solchen Anbindung anbieten, um eine sichere Cloud–Nutzung gewährleisten zu können.

prego. services

5. Security/Visibility – digitale Transformation und moderne, sichere Netzwerke

Das IT-Sicherheitsgesetz fordert ein Mindestmaß an IT-Security in kritischen Infrastrukturen. Büronetzwerke haben in der Regel den IT-Grundschutz oder branchenspezifische Regelwerke wie ISO27001, TR27016 usw. als Vorlage. Die digitale Transformation hat an Tempo zugelegt.

Wie setzen wir solche Themen konkret um?
Grundsätzlich kann das Sicherheitsniveau durch eine Risikoanalyse bewertet werden.
Danach müssen geeignete Maßnahmen folgen.
Wir bieten Risikoanalysen, Sicherheitsanalysen, Securitystrategien, Umsetzungs- und Architekturberatung, Netzwerkrealisierung und -betrieb.

6. Schnittstellen der Netzwerke öffnen sich

Je mehr digitale Kommunikationsbeziehungen über Unternehmensgrenzen hinweg abgewickelt werden, umso mehr Schnittstellen müssen aus den Netzwerken geöffnet werden: Prozessnetzwerke, Büronetzwerke, Leitstellennetzwerke.

Je mehr Zugangspunkte existieren, desto mehr „Löcher" werden für mögliche Cyber-Attacken geöffnet.

IT-Verantwortliche müssen dabei einerseits das Netzwerk nach außen öffnen, ohne andererseits die Sicherheit sensibler Daten zu gefährden. Hier braucht es die entsprechende maßgeschneiderte Security-Architektur.

Wie setzen wir solche Themen konkret um?
Wir haben jahrelange Erfahrung im laufenden Betrieb und der Absicherung von Schnittstellen zwischen Netzwerken mit unterschiedlichem Sicherheitsniveau. Zweistufige Firewall, auditfähiges Firewall-Regelwerk, Mikro-Segmentierung: All das sind Security-Architekturen, die von uns umgesetzt werden.

Haben Sie Fragen zu unserem Enterprise Network-Angebot?

Wir helfen Ihnen gerne weiter.

Kontakt

prego services GmbH
Neugrabenweg 4 · 66123 Saarbrücken
Franz-Zang-Straße 2 · 67059 Ludwigshafen
0681 95943-1265
vertrieb@prego-services.de
www.prego-services.de
info@prego-services.de

prego. services

Stand: 11/2018 v2